Courts affirm FBI use of mass-hacking tool to find child-porn suspects; The findings are the first in an uncharted and technologically complex area of the law.

Washington Post Blogs

January 29, 2016 Friday 10:55 PM EST

washingtonpost.com

Length: 809 words

Byline: Ellen Nakashima

Body

Over the past week, two federal judges have found that the government's use of software in a mass hacking of child-porn websites to identify users is constitutional.

The findings by judges in Tacoma, Wash., and Milwaukee are the first in an uncharted and technically complex area of law.

The two cases involved a child-porn website, Playpen, that was reachable only through the installation of special software called Tor, the world's most widely used tool to give users anonymity online.

Because users who gravitate to Playpen were able to hide their tracks using Tor, the FBI in both cases obtained search warrants to hack the website and surreptitiously place computer code, or malware, on computers logging into certain forums on the site. When a user logs in and clicks on the forum, the malware exploits a flaw in his browser, forcing his computer to reveal its true Internet protocol address.

The defendant in the Tacoma case, Keith Michaud, argued that by hacking a website and infecting possibly thousands of computers in unknown locations - the site had 215,000 members - the government's action violated the Fourth Amendment's requirement that a warrant ″particularly″ describe the place to be searched.

Michaud, who has been charged with receipt and possession of child pornography, also argued it amounted to a general warrant, a reference to the British practice during the Colonial era of allowing government searches without individualized suspicion.

But U.S. District Judge Robert J. Bryan, in the Western District of Washington, denied Michaud's motion to throw out his charges on constitutional grounds.

″Although the FBI may have anticipated tens of thousands of potential suspects as a result of deploying the ['Network Investigative Technique'], that does not [violate the Constitution] because it would be highly unlikely that Website A would be stumbled upon accidentally,″ Bryan said in an order issued Thursday.

″What was done here was ultimately reasonable,″ Bryan wrote. ″The [hacking] warrant was supported by probable cause and particularly described the places to be searched and the things to be seized.″

Michaud's defense attorney, Colin Fieman, took issue with the ruling. ″We have tremendous regard for Judge Bryan, but in this case respectfully and profoundly disagree with the court's decision not to suppress evidence seized as part of the FBI's operation of a massive child-pornography website and use of investigatory methods that we believe violate the Fourth Amendment and erode the privacy rights of everyone.″

In a separate but related case in Milwaukee, a judge similarly found that the FBI had probable cause to issue a warrant to deploy the malware - what the bureau calls the Network Investigative Technique (NIT) - and rejected the defendant's motion to dismiss the charges. That finding by Judge David E. Jones was disclosed by Justice Department trial attorney Keith Becker at a Jan. 22 hearing in Michaud's case, according to a transcript of the hearing. But Jones's report, which is a recommendation to the district judge, has not yet been made public.

Michaud also argued that the government violated Rule 41, a regulation established by the federal courts that requires that a warrant be deployed in the district in which it is issued. The NIT warrant in his case was issued in the Eastern District of Virginia. Michaud's computer was in Vancouver, Wash.

Bryan ruled that the warrant ″technically violates the letter, but not the spirit, of Rule 41.″ And the technical violation, he said, did not warrant suppression of the evidence.

The courts are in the process of weighing a change to Rule 41, which would make clear that a judge can issue a warrant to deploy a hacking tool in an unknown district to discover the location of a suspect's computer.

The technical complexity of the issue was evident in the Jan. 22 hearing in Michaud's case. At the hearing, Bryan spent some time trying to understand exactly how the NIT worked.

″When somebody got the authority to attach the NIT to the website, how do you do that? Does somebody sit down on a computer and make keystrokes to make that happen?″ he asked, according to the transcript.

When advised by Becker that the warrant explained the NIT's operation, Bryan replied: ″It doesn't explain the things I am asking about.″ The back-and-forth went on for some time when the judge decided it was time for a break.

But before breaking, he reiterated: ″I want to know what the user has to do to trigger this NIT, if anything. Then . . . the information that the NIT provides, how does [the FBI] get that? I suppose there is somebody sitting in a cubicle somewhere with a keyboard doing this stuff. I don't know that. It may be they seed the clouds, and the clouds rain information. I don't know that.″

The defendants in both cases plan to appeal.

ellen.nakashima@washpost.com

Classification

Language: ENGLISH

Publication-Type: Web Blog

Subject: PORNOGRAPHY (90%); CHILD PORNOGRAPHY (89%); LAW ENFORCEMENT (89%); JUDGES (89%); INVESTIGATIONS (89%); PROBABLE CAUSE (89%); SPECIAL INVESTIGATIVE FORCES (89%); DECISIONS & RULINGS (78%); LAWYERS (78%); JUSTICE DEPARTMENTS (78%); LITIGATION (78%); CONSTITUTIONAL LAW (77%); SEARCH WARRANTS (75%); LAW COURTS & TRIBUNALS (73%); EVIDENCE (73%); PRIVACY RIGHTS (71%); SEX OFFENSES (70%)

Industry: MALICIOUS SOFTWARE (90%); COMPUTER SOFTWARE (90%); COMPUTER NETWORK SECURITY (89%); WEBSITE FAILURES (78%); LAWYERS (78%); LITIGATION (78%); HIDDEN WEB (78%); NETWORK PROTOCOLS (68%)

Geographic: MILWAUKEE, WI, USA (92%); TACOMA, WA, USA (88%); WASHINGTON, USA (79%); WISCONSIN, USA (79%); UNITED STATES (92%)

Load-Date: January 29, 2016